Risk Checklist

Financial Institution

Holiday Fraud Prevention For Financial Institutions and Consumers

Fraud and scams are heightened during the holiday season due to increased spending and shopping, both online and in stores. Review these precautionary measures to help detect, prevent, and protect against fraudulent holiday attacks.

Allied Solutions

May 2021

Financial Institution Holiday Fraud Prevention Checklist:

- ☐ Educate cardholders about the heightened risk of attacks and scams during the holiday season, such as phishing attacks, scams where the consumer is asked to pay the scammer money and recruitment scams where the consumer is asked to pay a bit of money up front to earn more money later on.
  - If you are aware of a scam, place the scam on your website, in your newsletter and/or in the lobby of your branches to inform consumers.
  - Share information about scams with your employees.
  - Consider setting up a hot line for consumers to call if they are suspicious of any fraud activity.
- ☐ Validate if the fraud is "card-present" versus "card-not-present" to find out where the fraud is happening.
- ☐ Ensure you have comprehensive layers of security and authentication for both card-present and card-not-present transactions.

Visit our website for more risk education: ***alliedsolutions.net/resources***

- ☐ Consider immediately blocking and reissuing potentially compromised cards to prevent future risk.
- ☐ Recommend to staff and consumers to more closely and more frequently monitor ACH items, outgoing wires, and online transaction activity on all of their cards and accounts to look out for any unauthorized activity.
- ☐ Utilize communications tools to increase the stream of information to your staff and consumers about the increased likelihood of scams and attacks during the holiday season.
- ☐ Flag or block any unusual out-of-state card purchases. Inform consumers to alert you if they are traveling over the holidays, so that they are not affected by these preventative measures.
- ☐ Monitor any type of card fraud, especially online payment card fraud, to help identify a card breach. Look for a common point of compromise and report it to the fraud department at the card association (i.e. Visa or MasterCard) immediately.

- ☐ Ensure that your institution is receiving Visa alerts (CAMs) or MasterCard alerts regarding compromised cards and/or regarding information about the type of card data at risk (i.e. Track 1, Track 2, etc.).
- ☐ Determine if you will block and reissue or monitor compromised card numbers. (In cases where the full unaltered magnetic stripe has been compromised, it is strongly recommended to block and reissue the card data.)
- ☐ Contact cardholders directly to let them know when they are part of a breach.
- ☐ Share a message on your website or phone system with any updates about a widespread breach.
- ☐ Monitor PIN change activity. The criminal may make multiple attempts to perform a PIN change in order to obtain card data.
- ☐ Review daily dollar limits for signature, Internet, and PIN transactions and offer consumers the option to lower their daily card limits over the holiday season.
- ☐ Watch for multiple payments on the same day or within days of each other on credit card accounts and do not provide availability of a payment to the credit card holder until other payments clear.
- ☐ Watch for increased cash disbursements (advances) being requested on cards not issued by your financial institution.
- ☐ Utilize an anti-skimming device on your ATMs.
- ☐ Utilize multiple layers of authentication when validating and sending out ACH and wire transactions both online and in-person to help prevent any unauthorized withdrawals of consumers' funds.
- ☐ Perform a review of your fraud risk tools and programs to assess their effectiveness.
- ☐ Continue to enhance your fraud protection strategies and your fraud management systems to help prevent card exposure.

Consumer Holiday Scam Prevention Checklist:

- ☐ Place a credit freeze on your credit reports with all three credit bureaus: TransUnion, Experian, and Equifax.
- ☐ Sign up for free fraud alerts from credit bureaus.
- ☐ Take extra time to monitor accounts closely for any type of unauthorized activity.
- ☐ When shopping online, remember to exit the website.
- ☐ Only use a private network when shopping or performing account activity online.
- ☐ Check out sellers before purchasing items.
- ☐ Cover hand when entering PIN at a store or on an ATM.
- ☐ Watch merchants perform purchase sales to be on the lookout for any suspicious activity.
- ☐ Review card account transactions daily to uncover any unauthorized activity.
- ☐ Always save purchase receipts.
- ☐ Inform financial institution(s) of any travel activity.
- ☐ Consider requesting lower daily dollar limits on account transactions.
- ☐ Subscribe to fraud alerts.
- ☐ If contacted about card fraud, contact financial institution directly to confirm the fraud call's validity – DON'T EVER provide financial information to callers.

Contact us to receive more risk education and support: alliedsolutions.net/contact-us.

Allied Solutions
GROW, PROTECT AND EVOLVE YOUR BUSINESS.®

This checklist is for informational purposes only and is not to be considered legal advice.

975-R7-5/21